Chapter 3
Basic Installation and Configuration

This chapter describes how to set up your NETGEAR ProSafe Wireless Access Point 802.11g WG302 for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b or 802.11g wireless adapters to do such things as connect to the Internet, or access printers and files on your LAN.

Note: Indoors, computers can connect over 802.11g wireless networks at ranges of several hundred feet or more. This distance can allow for others outside your area to access your network. It is important to take appropriate steps to secure your network from unauthorized access. The WG302 Access Point provides highly effective security features which are covered in detail in "Understanding WEP/WPA Security Options" on page 3-15. Deploy the security features appropriate to your needs.

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the WG302 that conforms to the Observing Placement and Range Guidelines below.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or Cable/DSL gateway.
- One or more computers with properly configured 802.11b or 802.11g wireless adapters.

Observing Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless access point. The latency, data throughput performance, and notebook power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the WG302. For complete performance specifications, see Appendix A, "Specifications".

For best results, place your wireless access point:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.
- Putting the antenna in a vertical position provides best side-to-side coverage. Putting the antenna in a horizontal position provides best up-and-down coverage.
- If using multiple access points, it is better if adjacent access points use different radio frequency Channels to reduce interference. The recommended Channel spacing between adjacent access points is 5 Channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook computer.

Cabling Requirements

The WG302 Access Point connects to your LAN via twisted-pair Category 5 Ethernet cable with RJ-45 connectors.

Default Factory Settings

When you first receive your WG302, the default factory settings will be set as shown below. You can restore these defaults with the Factory Default Restore switch on the rear panel — see "WG302 front panel" on page 2-6.

FEATURE	FACTORY DEFAULT SETTINGS
User Name (case sensitive)	**admin**
Password (case sensitive)	**password**
Operating Mode	**Access Point**
Access Point Name	**netgearxxxxxx where xxxxxx are the last six digits of the wireless access point's MAC address**
Built-in DHCP client Built-in DHCP server	**DHCP client disabled** **DHCP server disabled**
IP Configuration (if DHCP server is unavailable)	**IP Address: 192.168.0.228** **Subnet Mask: 255.255.255.0** **Gateway: 0.0.0.0**
Network Name (SSID)	**NETGEAR**
Broadcast Network Name (SSID)	**Enabled**
802.11g Radio Frequency Channel	**11**
AutoCell RF Management AutoCell Enhanced RF Security 'stealth' mode	**Enabled** **Disabled**
WEP/WPA	**Disabled**
Restricting connectivity based on MAC Access Control List	**Disabled**
Spanning Tree Protocol	**Enabled**
Time Zone	**GMT**
Time Zone Adjust for Daylight Saving TIme	**Disabled**
SNMP	**Enabled but Trap forwarding is disabled**
Secure Telnet	**Enabled**
SugerG Mode	**Disabled**
WMM Mode	**Disabled**

Understanding WG302 Wireless Security Options

Your wireless data transmissions can be received well beyond your walls by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The WG302 Access Point provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

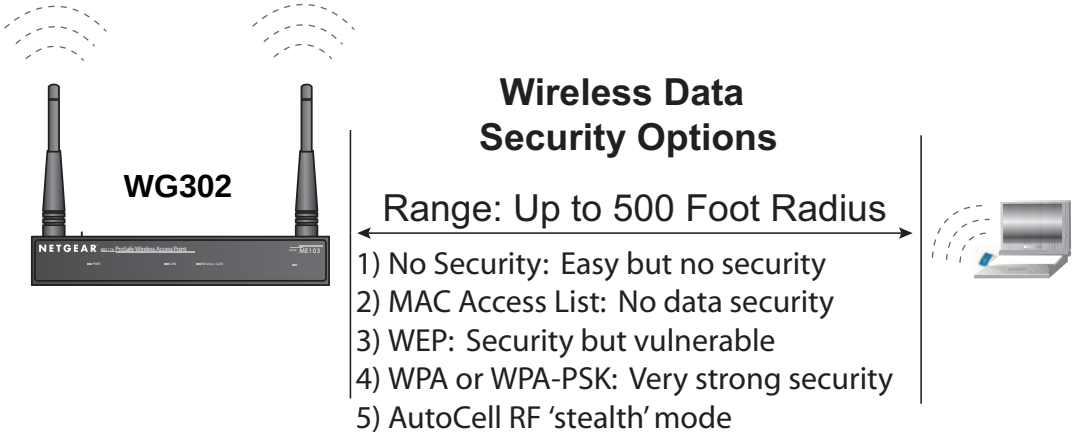
WG302
NETGEAR
Wireless Data
Security Options
Range: Up to 500 Foot Radius
1) No Security: Easy but no security
2) MAC Access List: No data security
3) WEP: Security but vulnerable
4) WPA or WPA-PSK: Very strong security
5) AutoCell RF 'stealth' mode

Figure 3-1: WG302 wireless data security options

There are several ways you can enhance the security of your wireless network:

- **Restrict Access Based on MAC address.** You can restrict access to only trusted PCs so that unknown PCs cannot wirelessly connect to the WG302. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network 'discovery' feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers.
- **Use WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

- **Use WPA, WPA-PSK, WPA2, or WPA2-PSK.** Wi-Fi Protected Access (WPA and WPA2) data encryption provides data security. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise. Because this is a new standard, wireless device driver and software availability may be limited.
- **Use AutoCell Enhanced RF Security 'Stealth Mode.'** In addition to standard encryption and security mechanisms such as WEP and WPA, the WG302 AutoCell feature provides self-organizing micro cells for an additional level of privacy for enterprises. In this mode, AutoCell shrinks the size of coverage to the minimum to reach clients but also shrinks the size of the beacons that access points use to announce their presence. This mode makes an enterprise wireless LAN nearly invisible to users outside an office building. AutoCell clients such as the NETGEAR WAG511 are highly-recommended for Enhanced RF Security.

Installing the WG302 Access Point

Before installing the NETGEAR ProSafe Wireless Access Point 802.11g WG302, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b or 802.11g wireless adapters will be able to communicate with computers on the Ethernet network. In order for this to work correctly, verify that you have met all of the system requirements, shown on page 2-5.

1 Set up the WG302 Access Point

Tip: Before mounting the WG302 in a high location, first set up and test the WG302 to verify wireless network connectivity.

a. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings.

b. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 for the Subnet Mask.

c. Connect an Ethernet cable from the WG302 to the computer.

d. Turn on your computer, connect the power adapter to the WG302 and verify the following:

   – The PWR power light goes on.

   – The LAN light of the wireless access point is lit when connected to a powered on computer.

2 CONFIGURE LAN AND WIRELESS ACCESS

a. Configure the WG302 Ethernet port for LAN access.

- Connect to the WG302 by opening your browser and entering *http://192.168.0.228* in the address field. A login window like the one shown below opens:

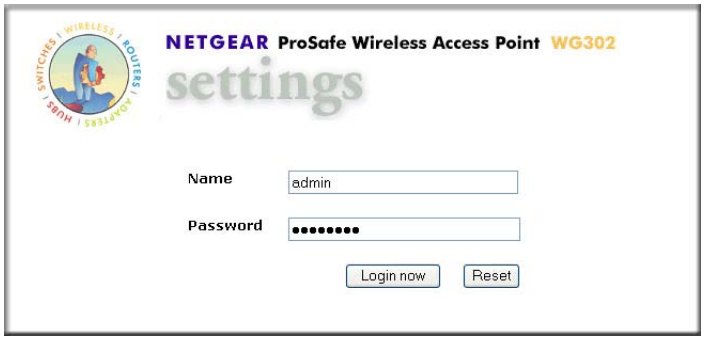

Figure 3-2: Login window

- When prompted, enter **admin** for the user name and **password** for the password, both in lower case letters.

- The Web browser will then display the WG302 settings page.

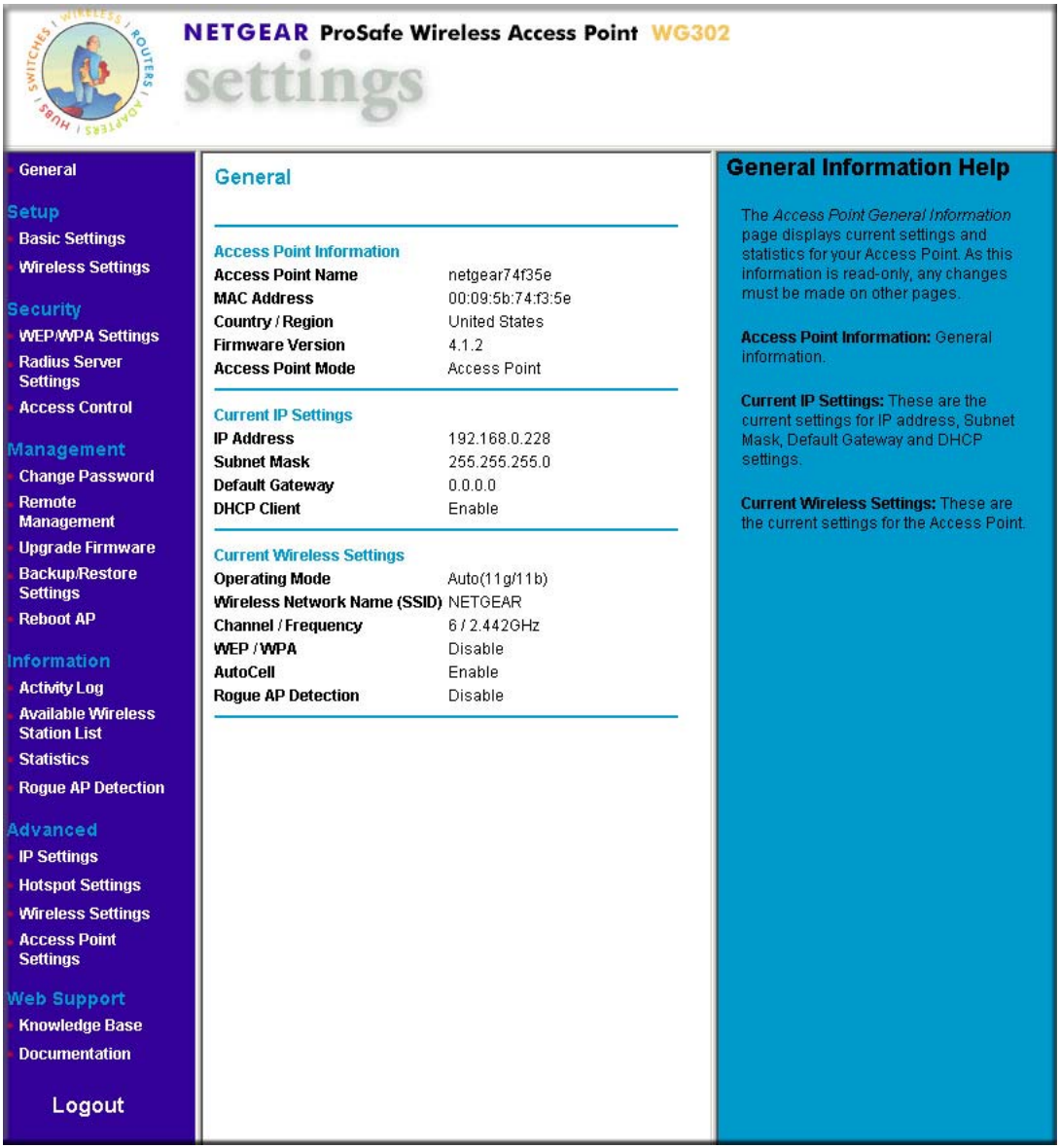

Figure 3-3: Login result: WG302 home page

– When the wireless access point is connected to the Internet, click the Knowledge Base or the Documentation link under the Web Support menu to view support information or the documentation for the wireless access point.

– If you do not click Logout, the wireless access point will wait 5 minutes after there is no activity before it automatically logs you out.

• Click the Basic Settings link to view the Basic Settings menu.

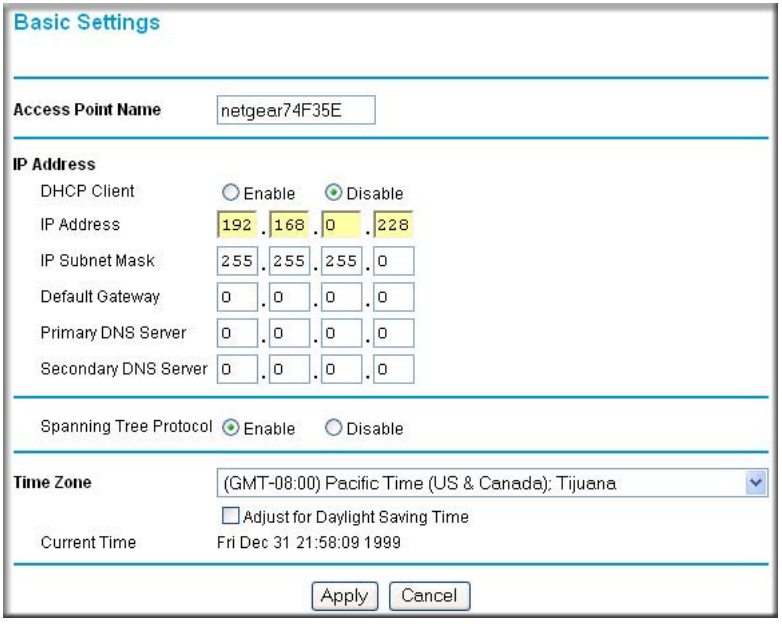

Figure 3-4: Basic Settings menu

• Configure the settings appropriate for your network.

b. Click the Wireless Settings link in the Setup section of the main menu to view the Wireless Settings menu.

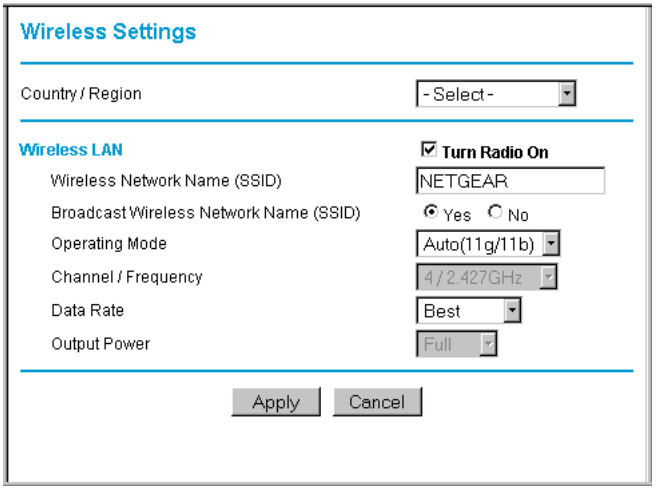

Figure 3-5: Basic Wireless Settings menu

c. Configure the wireless interface for wireless access. See the online help or the Understanding Basic Wireless Settings topic of this Reference Manual for full instructions.

Note: You must set the Regulatory Domain. It may not be legal to operate the wireless access point in a region other than one of those identified in this field.

Now that you have finished the setup steps, you are ready to deploy the WG302 in your network. If needed, you can now reconfigure the computer you used in step 1 back to its original TCP/IP settings.

3 Deploy the WG302 Access Point

a. Disconnect the WG302 and position it where you will deploy it. The best location is elevated, such as wall mounted or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.

b. Lift the antenna on either side so that they are vertical.

Note: Consult the antenna positioning and wireless mode configuration information in the Advanced Configuration chapter of the Reference Manual.

c. Connect an Ethernet cable from your WG302 Access Point to a LAN port on your router, switch, or hub.

Note: By default, WG302 is set to with the DHCP client disabled. If your network uses dynamic IP addresses, you will need to change this setting.

d. Connect the power adapter to the wireless access point and plug the power adapter in to a power outlet. The PWR, LAN, and Wireless LAN lights and should light up.

4 VERIFY WIRELESS CONNECTIVITY

Using a computer with an 802.11b or 802.11g wireless adapter with the correct wireless settings needed to connect to the WG302 (SSID, WEP/WPA, MAC ACL, etc.), verify connectivity by using a browser such as Netscape or Internet Explorer to browse the Internet, or check for file and printer access on your network.

Note: If you are unable to connect, see Chapter 6, "Troubleshooting."

How to Log In to the WG302 Using Its Default IP Address

1. 192.168.0.228 is the default IP address of your access point. The WG302 is set by default with the DHCP client disabled.

   Note: The computer you are using to connect to the WG302 should be configured with an IP address that starts with 192.168.0.x and a Subnet Mask of 255.255.255.0.
2. Open a Web browser such as Internet Explorer or Netscape Navigator.
3. Connect to the WG302 by entering its default address of *http://192.168.0.228* into your browser.
4. A login window like the one shown below opens:

Figure 3-6: Login window

Log in use the default user name of **admin** and default password of **password**.

Once you have entered your access point name, your Web browser should automatically find the WG302 Access Point and display the home page, as shown in "Login result: WG302 home page" on page 3-7.

Using the Basic IP Settings Options

The Basic IP Settings menu is under the Basic heading of the main menu. Use this menu to configure DHCP, static IP, and access point access point name settings.

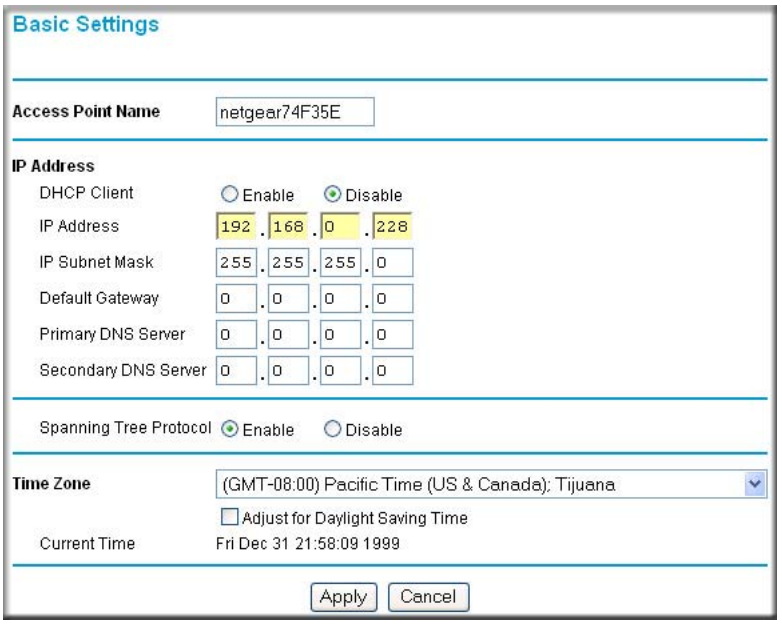

Figure 3-7: IP Settings menu

- **Access Point Name (NetBIOS)**

  Enter a new name for the wireless access point and click Apply to save your changes.

- **The IP Address**

  The wireless access point is shipped preconfigured with its DHCP client disabled and with the following private static IP addresses:

  – IP Address — 192.168.0.228

  – IP Subnet Mask — 255.255.255.0

  – Gateway — 0.0.0.0

  – Primary and Secondary DNS Servers — 0.0.0.0

  If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu. These settings are only required if the “Use this IP address” radio button is chosen. Remember to click Apply to save your changes.

- **Spanning Tree Protocol**

  Spanning Tree Protocol in enabled by default for the wireless access point. This provides network traffic optimization in settings with multiple WG302 Access Points.

- **Time Zone**

  Select the time zone location for your setting.

  Note: You must have an Internet connection to get the current time.

Understanding Basic Wireless Settings

To configure the wireless settings of your wireless access point, click the Wireless Settings link in the Basic section of the main menu of the browser interface. The Basic Wireless Settings menu will appear, as shown below.

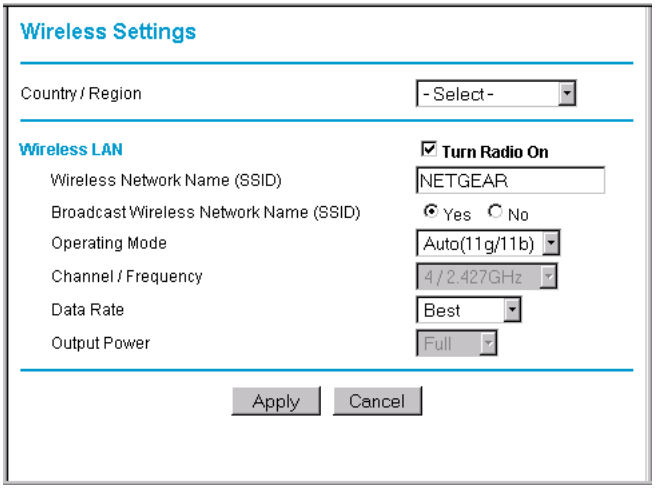

Figure 3-8: Basic Wireless Settings menu

The Basic Wireless Settings menu options are discussed below:

- **Country/Region.** This field identifies the region where the WG302 can be used. It may not be legal to operate the wireless features of the wireless access point in a region other than one of those identified in this field. There is no default country domain, and the channel is set to 11. Unless a country domain is selected, the channel cannot be changed.

- **Turn Radio On**. On by default, you can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.
- **Wireless Network Name (SSID).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in a particular wireless network will need to use the SSID. The WG302 default SSID is: **NETGEAR**.
  - A group of Wireless Stations and a single access point, all using the same ID (SSID), form a Basic Service Set (BSS).
  - Using the same SSID is essential. Devices with different SSIDs are unable to communicate with each other. However, some access points allow connections from wireless stations which have their SSID set to “any” or whose SSID is blank (null).
  - A group of wireless stations and multiple access points, all using the same ID (ESSID), form an Extended Service Set (ESS).
  - Different access points within an ESS can use different channels. To reduce interference, it is recommended that adjacent access points *should* use different channels.
  - As wireless stations physically move through the area covered by an ESS, they will automatically change to the access point which has the least interference or best performance. This capability is called roaming.

    Note: The AutoCell feature enhances the roaming, interference, and channel selection of an extended wireless network.
- **Broadcast Wireless Network Name (SSID).** This field lets you turn off the SSID broadcast. If you turn off the SSID broadcast, only stations that know the SSID will connect. Disabling SSID broadcast somewhat hampers the wireless network ‘discovery’ feature of some products. The default is to enable SSID broadcast.

Note: Broadcast Wireless Network Name (SSID) is automatically turned off when you select the AutoCell Enhanced RF Security option in the advanced wireless settings page.

- **Operating Mode**. Select the desired wireless operating mode. The options are:
  - Auto (11g/b) – Both 802.11g and 802.11b wireless stations can be used. This is the default.
  - 11g Only - Only 802.11g wireless stations can be used. This is required for 108 Mbps data rate operation.

  - 11b Only - All 802.11b wireless stations can be used. 802.11g wireless stations can still be used if they can operate in 802.11b mode.

- **Channel.** This field identifies which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems or setting up the WG302 near another access point. See "Wireless Channels" on page B-7 for more information on wireless channels.

Note: Channel selection is automatically adjusted by AutoCell when the Auto RF Management option is enabled. The default setting is for the AutoCell Auto RF Management option to be enabled.

  - Access points use a fixed channel. You can select the channel used. This allows you to choose a channel which provides the least interference and best performance. In the USA and Canada, 11 channels are available.

    Note: Channel 6 is required for 108 Mbps data rate.

  - If using multiple access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).

  - In "Infrastructure" mode, wireless stations normally scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can only happen when the various access points are using the same SSID.

- **Data Rate**. Shows the available transmit data rate of the wireless network. 108 Mbps is only available when the operating mode is 802.11g only and the channel is 6. The default is Best.

- **Output Power**. Set the transmit signal strength of the access point. The options are full, half, quarter, eighth, and min. Decrease the transmit power if more than one AP is colocated using the same channel frequency. The default is Full.

Note: Output power is automatically adjusted by AutoCell when the Auto RF Management option is enabled. The default setting is for the AutoCell Auto RF Management option to be enabled.

Understanding WEP/WPA Security Options

The table below identifies the various WEP/WPA security options. A full explanation of these standards is available in Appendix B, "Wireless Networking Basics".

Figure 3-9: Wireless Security Settings

The WEP/WPA settings are explained as follows:

- **Network Authentication**: Specifies the Authentication type used. The default is Open System. Select the desired option:
  - **Open System**: If selected, you have the option of using WEP encryption, or no encryption.
  - **Shared Key**: If selected, you must use WEP; at least one shared key must be entered.
  - **Legacy 802.1x**: If selected, you must configure the Radius Server Settings Screen.
  - **WPA-PSK**: If selected, you must use TKIP encryption, and enter the WPA passphrase (Network key).
  - **WPA with Radius**: If selected, you must configure the Radius Server Settings Screen.
  - **WPA2-PSK**: WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and enter the WPA passphrase (Network key).

  - **WPA-PSK and WPA2-PSK**: This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES. The WPA passphrase (Network key) must also be entered.
  - **WPA2 with Radius**: WPA2 is a later version of WPA. Only select this if all clients support WPA2. If selected, you must use AES encryption, and configure the Radius Server Settings Screen.
  - **WPA and WPA2 with Radius**: This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, encryption must be TKIP + AES, and you must also configure the Radius Server Settings Screen.

  Note: All options are available if using Access Point mode. In other modes (e.g. Repeater or Bridge) some options may be unavailable.

- **Data Encryption**: Select the desired option. The available options depend on the Network Authentication setting above (otherwise, the default is None). The supported options are:
  - **None**: No encryption is used.
  - **64 bits WEP**: Standard WEP encryption, using 40/64 bit encryption.
  - **128 bits WEP**: Standard WEP encryption, using 104/128 bit encryption.
  - **152 bits WEP**: Proprietary mode that will only work with other wireless devices that support this mode.
  - **TKIP**: This is the standard encryption method used with WPA.
  - **AES**: This is the standard encryption method for WPA2. Some clients may support AES with WPA, but this is not supported by this Access Point.
  - **TKIP + AES**: This setting allows both WPA and WPA2 to be supported. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.
- **Passphrase**: To use the passphrase to generate the WEP keys, enter a passphrase and click **Generate Keys**. You can also enter the keys directly. These keys must match the other wireless stations.
- **Key 1, Key 2, Key 3, Key 4**: If using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys can only be used to decrypt received data.
- **WPA Passphrase (Network Key)**: If using WPA-PSK, enter the passphrase here. All wireless stations must use the same passphrase (network key). The network key must be from 8 to 63 characters in length.
- **Wireless Client Security Separation**: If enabled, the associated wireless clients will not be able to communicate with each other. This feature is intended for hotspots and other public access situations. The default is Disabled.

Before You Change the SSID and WEP Settings

For a new wireless network, print this form and fill in the parameters. For an existing wireless network, get the settings from the person who set up or is responsible for the network. Be sure to set the Regulatory Domain correctly as the first step. Store this information in a safe place.

- **SSID*:*** The Service Set Identification (SSID) identifies the wireless local area network. NETGEAR is the default WG302 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

  SSID: _____

  Note: The SSID in the wireless access point is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID:
- **Authentication**

  Circle one: Open System or Shared Key. Choose "Shared Key" for more security.

  Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key and have the same keys in the same positions as those in the WG302.
- **WEP Encryption Keys**

  For all four 802.11b keys, choose the Key Size. Circle one: 64, 128, or 152 bits

  Key 1: _____

  Key 2: _____

  Key 3: _____

  Key 4: _____
- **WPA-PSK (Pre-Shared Key)**

  Record the WPA-PSK key:

  Key: _____

  WPA2-PSK (Pre-Shared Key)

  Record the WPA2-PSK key:

  Key: _____
- **WPA RADIUS Settings**

  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____
- **WPA2 RADIUS Settings**

  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server Name/IP Address: Primary _____ Secondary _____

  Port: _____

  Shared Secret: _____

Use the procedures described in the following sections to configure the WG302.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in to the WG302 using its default address of *http://192.168.0.228* or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever password you set up.
2. Click the Wireless Settings link in the main menu of the WG302.
3. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

   Note: The SSID of any wireless access adapters must match the SSID you configure in the NETGEAR ProSafe Wireless Access Point 802.11g WG302. If they do not match, you will not get a wireless connection to the WG302.
4. Select the Country/Region in which the wireless interface will operate.
5. Set the Channel. It should not be necessary to change the wireless channel unless you notice interference problems or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your wireless access point. For more information on the wireless channel frequencies see "Wireless Channels" on page B-7.
6. For initial configuration and testing, leave the Wireless Card Access List set to "Everyone" and the Encryption Strength set to "Disabled."
7. Click Apply to save your changes.

Note: If you are configuring the WG302 from a wireless computer and you change the SSID, channel, or security settings, you will lose your wireless connection when you click Apply. You must then change the wireless settings of your computer to match the new settings.

8. Configure and test your PCs for wireless connectivity.

   Program the wireless adapter of your PCs to have the same SSID and channel that you configured in the WG302. Check that they have a wireless link and are able to obtain an IP address by DHCP from the WG302.

Once your PCs have basic wireless connectivity to the WG302, you can configure the advanced wireless security functions.

How to Restrict Wireless Access by MAC Address

To restrict access based on MAC addresses, follow these steps:

1. Log in to the WG302 using its default address of *http://192.168.0.228* or at whatever IP address the unit is currently configured. Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.

> **Note:** When configuring the WG302 from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.

2. From the Security menu, click the Access Control link to display the Access Control List menu shown below.

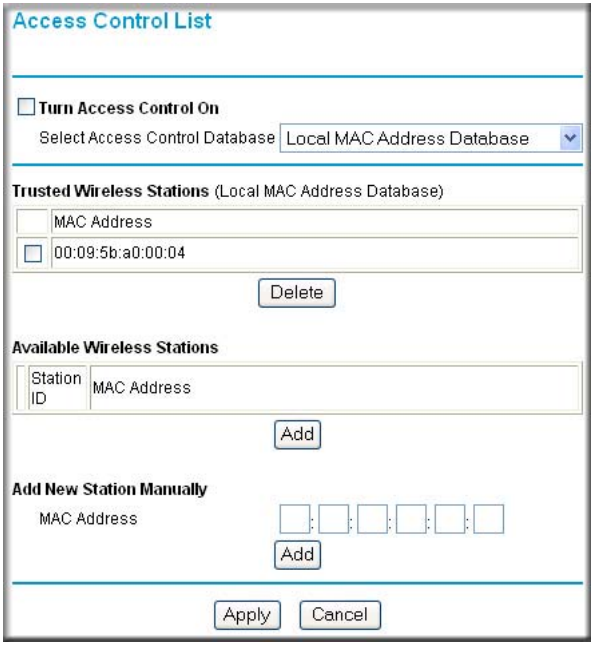

Figure 3-10: Access Control List menu

3. Select the Turn Access Control On check box.

4. Choose to use the local MAC address database stored on the access point, or use the RADIUS MAC address database stored on a RADIUS server. If you choose the RADIUS MAC Address Database, you must configure the RADIUS Server Settings first.
5. Then, either select from the list of available wireless cards the WG302 has found in your area, or enter the MAC address and device name for a device you plan to use. You can usually find the MAC address printed on the wireless adapter.
6. Click **Add** to add the wireless device to the access list. Repeat these steps for each additional device you want to add to the list.
7. Be sure to click **Apply** to save your wireless access control list settings.

Now, only devices on this list will be allowed to wirelessly connect to the WG302.

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in to the WG302 using its default address of *http://192.168.0.228* or at whatever IP address the unit is currently configured Use the default user name of **admin** and default password of **password**, or whatever LAN address and password you have set up.
2. Click the WEP/WPA Settings link in the main menu of the WG302.

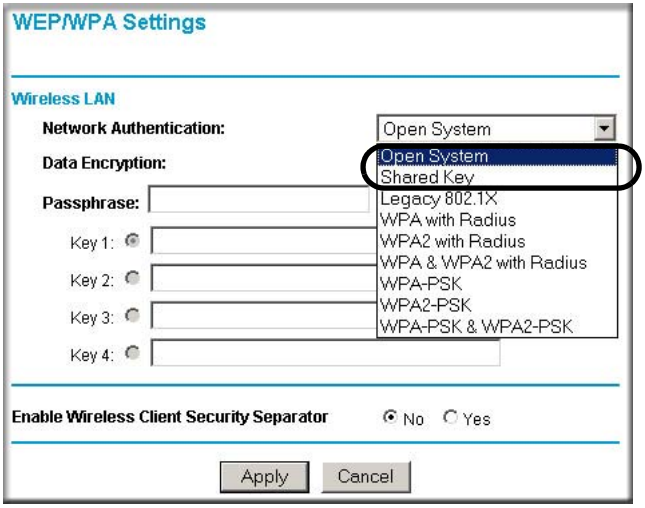

Figure 3-11: Wireless Settings menu

3. Choose Open System or Shared Key authentication.

4. Select encryption strength.
5. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
   - Automatic - enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
   - Manual - enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)
     Select which of the four keys will be the default.

   See "Overview of WEP Parameters" on page B-5 for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.
6. Click **Apply** to save your settings.

Note: If you use a wireless computer to configure WEP settings, you will be disconnected when you click Apply. Reconfigure your wireless adapter to match the new settings or access the wireless access point from a wired computer to make any further changes.

How to Configure WPA with Radius

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.228* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

2. Click **Radius Server Settings** in the Security menu.

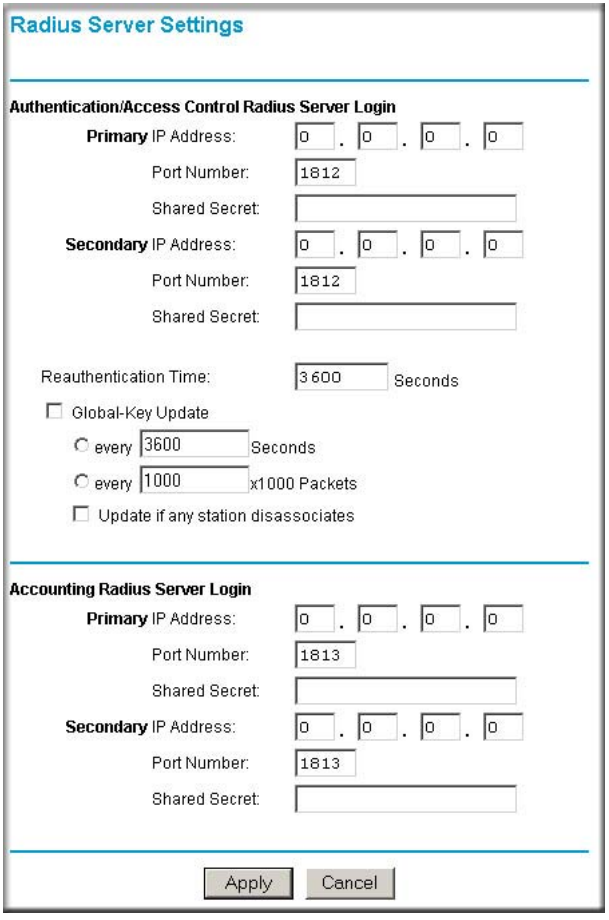

Figure 3-12: Radius Server Settings

3. Enter the Radius settings.

   - **Authentication/Access Control Radius Server Configuration**: This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
   - **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
   - **Port Number**: Port number of the Radius Server. The default is 1812.

- **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
- **Re-authentication Time**: The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.
- **Global-key Re-Key Time**: Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
- **Update if any station disassociates**: Check on this option to refresh global key when any stations disassociated with wireless Access Point.
- **Accounting Radius Server Configuration**: This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
- **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
- **Port Number**: Port number of the Radius Server. The default is 1813.
- **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

4. Click **Apply** to save your settings.
5. Click **WEP/WPA Settings** in the Security menu.

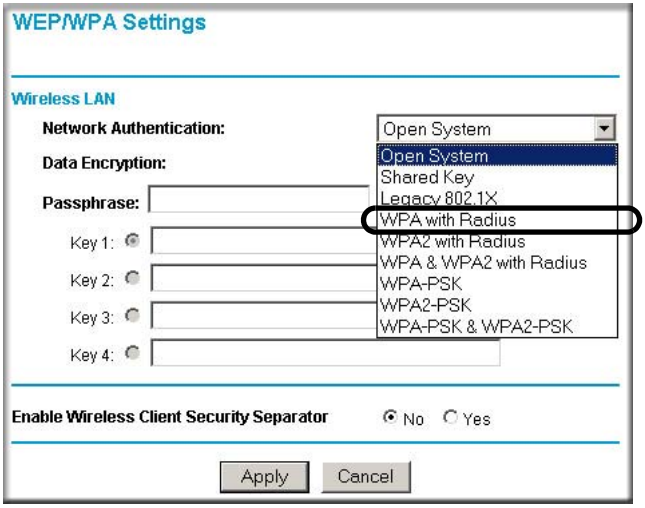

Figure 3-13: Wireless Settings menu

6. Choose **WPA with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA-PSK

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

To configure WPA-PSK, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.228* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **WEP/WPA Settings** in the Security menu of the WG302.

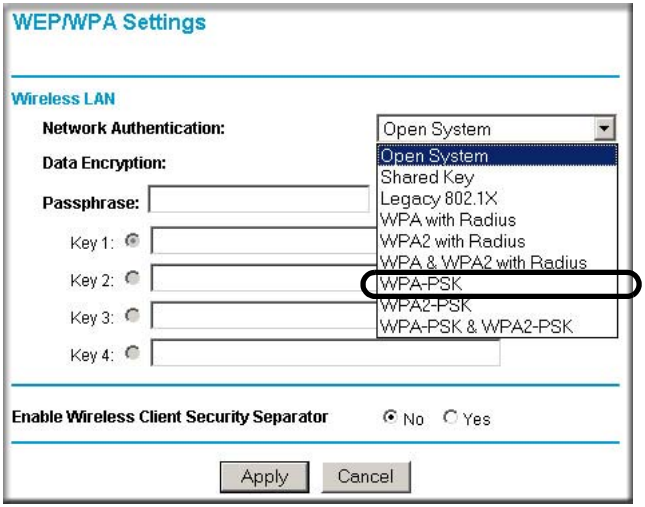

Figure 3-14: WEP/WPA Settings menu

3. Choose **WPA-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.

How to Configure WPA2 with Radius

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Radius Server Settings** in the Security menu.

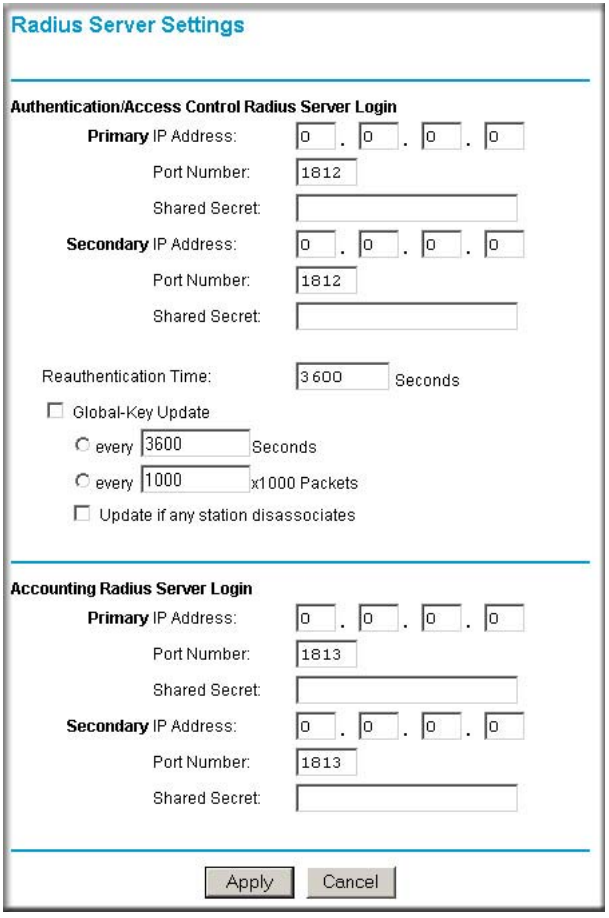

Figure 3-15: Radius Server Settings menu

3. Enter the Radius settings.

   - **Authentication/Access Control Radius Server Configuration**: This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
   - **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
   - **Port Number**: Port number of the Radius Server. The default is 1812.
   - **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
   - **Re-authentication Time**: The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.
   - **Global-key Re-Key Time**: Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
   - **Update if any station disassociates**: Check on this option to refresh global key when any stations disassociated with wireless Access Point.
   - **Accounting Radius Server Configuration**: This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
   - **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
   - **Port Number**: Port number of the Radius Server. The default is 1813.
   - **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

4. Click **Apply** to save your settings.

5. Click **WEP/WPA Settings** in the Security menu.

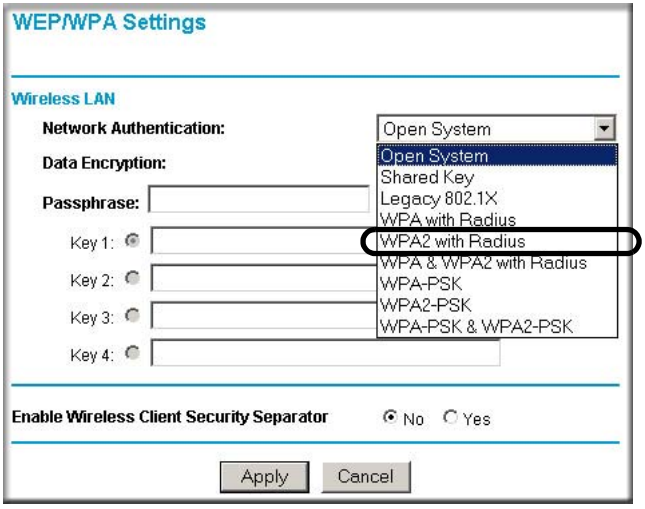

Figure 3-16: WEP/WPA Settings menu

6. Choose **WPA2 with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA2-PSK

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA2-PSK, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

2. Click **WEP/WPA Settings** in the Security menu of the WG302.

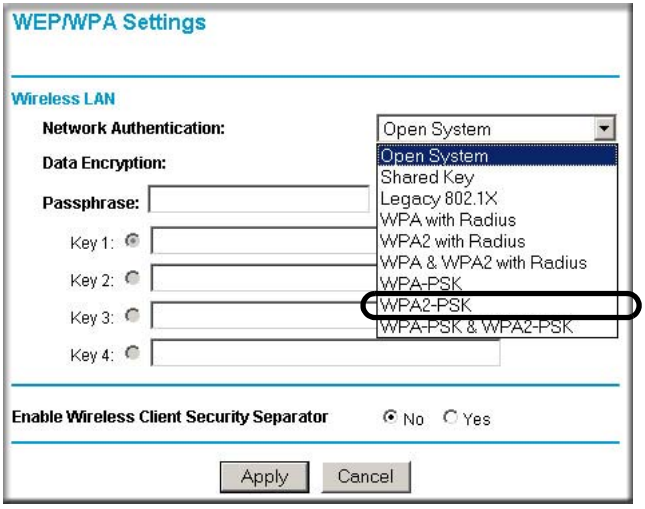

Figure 3-17: WEP/WPA Settings menu

3. Choose **WPA2-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.

How to Configure WPA and WPA2 with Radius

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA and WPA2, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click **Radius Server Settings** in the Security menu.

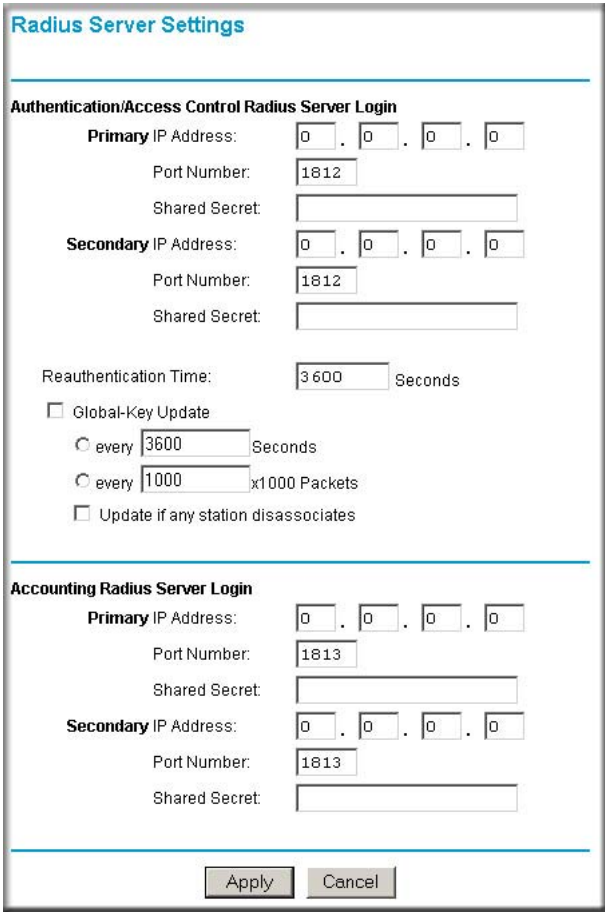

Figure 3-18: Radius Server Settings menu

3. Enter the Radius settings.

   - **Authentication/Access Control Radius Server Configuration**: This configuration is required for authentication using Radius. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server
   - **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
   - **Port Number**: Port number of the Radius Server. The default is 1812.
   - **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.
   - **Re-authentication Time**: The time interval in seconds after which the supplicant will be authenticated again with the Radius Server. The default is 3600 seconds.
   - **Global-key Re-Key Time**: Check on this option to enable Re-keying of Global Key. The Global Key Re-Key can be done based on time interval in seconds or number of packets exchanged using the global key. The default is 3600 seconds.
   - **Update if any station disassociates**: Check on this option to refresh global key when any stations disassociated with wireless Access Point.
   - **Accounting Radius Server Configuration**: This configuration is required for accounting using Radius Server. IP Address, Port No. and Shared Secret is required for communication with Radius Server. A Secondary Radius Server can be configured which is used on failure on Primary Radius Server.
   - **IP Address**: The IP address of the Radius Server. The default is 0.0.0.0.
   - **Port Number**: Port number of the Radius Server. The default is 1813.
   - **Shared Secret**: This is shared between the Wireless Access Point and the Radius Server while authenticating the supplicant.

4. Click **Apply** to save your settings.

5. Click **WEP/WPA Settings** in the Security menu.

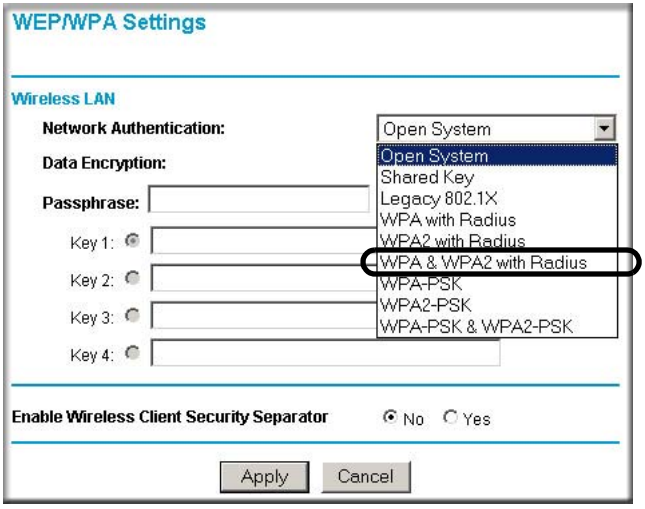

Figure 3-19: WEP/WPA Settings menu

6. Choose **WAP and WPA2 with Radius** from the list.
7. Click **Apply** to save your settings.

How to Configure WPA2-PSK and WPA2-PSK

Note: Not all wireless adapters support WPA. Furthermore, client software is required on the client. Windows XP and Windows 2000 with Service Pack 3 do include the client software that supports WPA. Nevertheless, the wireless adapter hardware and driver must also support WPA. Consult the product document for your wireless adapter and WPA client software for instructions on configuring WPA settings.

Note: Not all wireless adapters support WPA2. Furthermore, client software is required on the client. Make sure your client card supports WPA2. Consult the product document for your wireless adapter and WPA2 client software for instructions on configuring WPA2 settings.

To configure WPA-PSK and WPA2-PSK, follow these steps:

1. Log in at the default LAN address of *http://192.168.0.229* with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.

2. Click **WEP/WPA Settings** in the Security menu of the WG302.

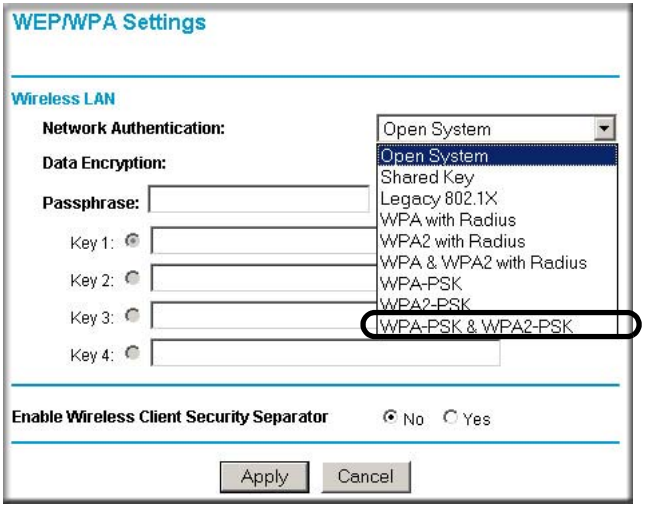

Figure 3-20: WEP/WPA Settings menu

3. Choose **WPA-PSK and WPA2-PSK** from the list.
4. Enter the pre-shared key passphrase.
5. Click **Apply** to save your settings.